



DEPARTMENT OF THE NAVY
NAVAL FACILITIES ENGINEERING COMMAND
1322 Patterson Ave., SE Suite 1000
Washington, DC 20374-5065

IN REPLY REF TO
NAVFACINST 5239.1B
NAVFAC CIO
05 APRIL 2000

NAVFAC INSTRUCTION 5239.1B

From: Commander, Naval Facilities Engineering Command

Subj: SECURITY REQUIREMENTS AND RESPONSIBILITIES FOR INFORMATION TECHNOLOGY

Ref: (a) OPNAVINST 5239.1B (DON Information Assurance Program)
(b) Public Law 100-235 (Computer Security Act of 1987)
(c) DOD Directive 5200.28 (Security Requirements for Automated Information Systems (AISs))
(d) SECNAVINST 5239.3 (DON Information System Security (INFOSEC) Program)

Encl: (1) Information System Security Policy and Responsibilities

1. Purpose. The purpose of this instruction is:

a. to ensure compliance with Department of Defense (DOD), Department of the Navy (DON) information assurance and information system security requirements,

b. to identify information assurance and information system security responsibilities for the Naval Facilities Engineering Command (NAVFACENGCOM) and its subordinate commands and activities, and

c. to highlight and provide guidance in specific areas.

2. Cancellation. This instruction supersedes and replaces NAVFACINST 5239.1 of March 2, 1993.

3. Scope. This instruction applies to all commands and activities of the Naval Facilities Engineering Command and all information technology therein.

4. Objective. The objective of this instruction is to provide centralized guidance and uniform information system (aka automated information system (AIS)/information technology and information assurance (IA)) security policy. This instruction defines information system security reporting requirements for the command and all subordinate commands and activities.

5. Background. Reference (a) established requirements for the DON Information Assurance Security Program. References (b) and (c) increased the emphasis and responsibility for AIS security, prompting reference (d). The information technology/system objective for each NAVFACENGCOM command/activity is to establish and maintain an effective Risk Management Program and achieve full accreditation for all information systems (i.e. applications), networks and computer resources based on the results of the information security accreditation process.

6. Definitions. Definitions applicable to this instruction are contained in Appendix A of enclosure (1).

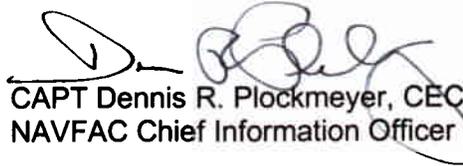
7. Policy. All NAVFACENGCOM commands and activities will establish and maintain an Information System Security Program in accordance with this instruction and references (a) through (d). The roles and responsibilities related to information technology/system security are included in enclosure (1).

8. Action.

a. Activities should continue the accreditation process as outlined in reference (a) while emphasizing information system accreditation as addressed in references (c) and (d). In instances where guidance in reference (d) conflicts with guidance in reference (a), reference (d) will take precedence.

b. The Chief Information Officer (CIO) will exercise oversight of the Information System Security Program through the command's inspection process.

9. Reporting. The Chief Information Officer (CIO) initiated intranet applications to support the Information System Security Program and to provide summaries of the command's information assurance and information system security posture. All NAVFACENGCOM commands and activities will maintain their own information within these applications in accordance with enclosure (1).


CAPT Dennis R. Plockmeyer, CEC, USN
NAVFAC Chief Information Officer

Distribution:

EFDs
EFAs
PWCs
NFESC
SLC
COMNAVFACENGCOM DETs

Information System Security Policy and Responsibilities

1. **Information System Security Policy.** Each NAVFACENGCOCOM Commander or Commanding Officer, and his/her Information System Security Manager (ISSM) will take the necessary steps to provide and document an adequate level of security for all information technology resources (i.e., information systems/applications, networks, etc.) under their cognizance. The decision to implement information system security countermeasures will be based upon security policies and procedures promulgated by this instruction and directives from higher authority. ISSMs are responsible for executing the Information System Security Program throughout the command. The ISSMs are responsible for reporting information assurance/information system security status and/or compliance using the Information Assurance/Information System Security intranet applications (URL:

<http://navfacilitator.navy.mil/cio/security.htm>). These applications are as follows:

- Information Assurance Training (End User and System Administrator)
- Information System Security Accreditation
- Information Assurance Vulnerability Alerts
- Information Operations Conditions
- Information System Security Incident Reporting
- Excessing Information Technology Resources

a. When processing classified information, activities must comply with DOD/DON information system security policy/instructions. For a complete/current listing of DOD/DON information security policy/instructions see Internet URL: <http://infosec.nosc.mil/CERTIFY/index.html>

b. NAVFACENGCOCOM Commanders and Commanding Officers shall enforce the policy for the management and use of proprietary software. Proprietary software shall be used in a manner consistent with the manufacturer's license agreement. The U.S. Government has no general exemption from copyright infringement liability. If an employee violates copyright law or other conditions of a software licensing agreement, disciplinary action may be taken. Employees who violate NAVFACENGCOCOM policy on copyright issues or who direct others to violate that policy are not considered acting in their official capacity and may be held personally liable for civil damages resulting from copyright infringement. SECNAVINST 5870.5 addresses permission to copy materials subject to copyright.

c. All computer resources that process or handle classified information, information critical for the command's mission, or sensitive unclassified information shall implement Class C2 Controlled Access Protection (CAP) functionality or appropriate security features above C2 as defined in the DOD 5200.28-STD (DOD Trusted Computer System Evaluation Criteria), unless directed otherwise by higher authority. Class C2 protection provides for discretionary access control, memory clearing before reuse, individual accountability and audit trails. All commands/ activities not meeting the C2 CAP requirement must issue a CAP waiver.

d. To ensure compliance with the information system security policies throughout the life cycle of an information system, network or other computer resource, developing activities will ensure the early and continuous involvement of the users, security staff, process owners and the Designated Approval Authority (DAA) in defining and implementing security requirements. Acquisition and procurement specifications must identify security requirements to the maximum extent possible. Computer security will be built into systems so that user responsibility to develop security procedures and controls for their system is minimized.

e. Labeling of data stored on magnetic media is required in controlled access areas (areas which handle/process classified data/information) and shall be in accordance with GSA, Information Security Oversight Office (ISOO) guidelines utilizing the following standard forms (labels):

FORM NUMBER	TITLE	STOCK NUMBER
SF 706	TOP SECRET label	SF 706:7540-01-207-5536
SF 707	SECRET label	SF 707:7540-01-207-5537
SF 708	CONFIDENTIAL label	SF 708:7540-01-207-5538
SF 709	CLASSIFIED label	SF 709:7540-01-207-5540
SF 710	UNCLASSIFIED label	SF 710:7540-01-207-5539
SF 711	Data Descriptor label	SF 711:7540-01-207-5541

These labels may be ordered from GSA using FEDSTRIP/MILSTRIP procedures. The SF 709, CLASSIFIED label, shall only be used when the output is classified but the level of classification has not yet been determined. UNCLASSIFIED labels shall be utilized in any environment where classified information of any level is stored or processed in the same area as unclassified data. Color-coded diskettes may be used, but their use does not replace or eliminate the requirement for standard labels. Printed reports shall be labeled in accordance with OPNAVINST 5510.1H.

2. Information System Security Responsibilities. The three principal participants in information system security are the Designated Approving Authority (DAA), the Information System Security Manager (ISSM) and the end user.

a. Designated Approving Authority (DAA). Unless otherwise designated, the Designated Approving Authority (DAA) for NAVFACENGCOM commands/activities is the Commanding Officer. The DAA is responsible for formally granting authority to operate information technology resources/systems based upon an acceptable level of risk, as recommended by the Information System Security Manager (ISSM). DAAs shall review and approve security safeguards and countermeasures for information technology and issue accreditation statements, to include all information technology resources under the DAA's jurisdiction, based on the acceptability of the security safeguards and countermeasures.

b. Information System Security Manager (ISSM). The ISSM shall be appointed by the DAA in writing. The ISSM will:

- (1) Identify security deficiencies and, if these deficiencies are serious enough to preclude accreditation, take appropriate corrective action to achieve an acceptable level of security.
- (2) Ensure all safeguards and countermeasures required to maintain an acceptable level of risk are implemented and maintained.
- (3) Ensure accompanying security staff (i.e., Network Security Officer (NSO), System Administrator(s), Information System Security Officer(s) (ISSO), etc.) is formally appointed and receives formal INFOSEC training to carry out the duties of their assigned function.
- (4) Ensure a continuing risk management process is in effect to minimize the potential for unauthorized disclosure of sensitive information, modification or destruction of assets, or denial of service.
- (5) Ensure process/data ownership is established/maintained for each information system, to include accountability, access rights, and special handling requirements.
- (6) Ensure the command/activity network and all stand-alone systems follow the least privileged principle, providing users the most restrictive set of privileges needed for the performance of authorized tasks. Each user is granted access to only that information to which the user is entitled by virtue of security clearance or formal access approval and only the resources necessary to perform assigned functions. In the absence of a specific positive grant of access, user access defaults to no access. The application of this principle limits the damage that can result from accident, error, or unauthorized use. For stand-alone microcomputers, physical access and magnetic media storage procedures should be addressed in respect to data sensitivity.
- (7) Consider information system security policies throughout the life cycle of all information technology (i.e., network, information system, etc.) from the beginning of concept development through design, development, deployment, acquisition, operation and maintenance until replacement or disposal.
- (8) Be responsible for determining and executing contingency plan(s) for all acquired information technology (i.e., network, information system, etc.).
- (9) Ensure that all employees having access to information technology actively participate in information technology/system security education and user awareness training programs in accordance with Public Law 100-235 (the Computer Security Act of 1987).
- (10) Assist the Physical Security Officer in the implementation/operation of the Public Key Infrastructure (PKI) requirements/policy.

c. Information System User(s). Information technology/system users shall:

- (1) Use the technology/system as intended, complying with DOD/DON and Command information system security and information technology policy.
- (2) Attend user awareness training programs in accordance with Public Law 100-235 (the Computer Security Act of 1987).

APPENDIX A

DEFINITIONS

Accreditation. The formal management authorization for operation of a specific business system application, network or computer resource, based on the results of a security certification and risk assessment. It is a formal declaration by the Designated Approving Authority (DAA) that the information technology/system is approved to operate in a particular security environment meeting a prescribed set of security requirements.

Activity Information System Security Incident. Information system security incidents are events that have actual or potential adverse effects on information systems. Some examples of adverse effects are as follows:

- Unauthorized Access (including intrusions to the NAVFAC Intranet)
- Denial of service/access
- Loss of data

Activity Information System Security Plan (AISSP). A required document used to establish and/or update the activity information system security program. It should promulgate information system security policy and provide guidelines to be used by the activity (i.e., document the current information system security environment, establish program objectives, and outline a plan of action and milestones for to achieve full accreditation).

Information Assurance (IA). Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information System (IS). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.

Certification. This is the formal technical evaluation of security features and other safeguards, made in support of the accreditation process, which establishes the extent to which a specific application of an information system, network or computer resource meets a set of specified technical security requirements.

Designated Approving Authority (DAA). Unless otherwise designated, the commanding officer is the DAA and is the authority to decide that an information technology, network and/or computer resource may operate based on an acceptable level of risk considering the operational need for, and threats to, the system; and is responsible for issuing an accreditation statement that records the decision.

Information System Security Posture Report. A NAVFACENGCOM Intranet application that displays the command's information system security posture. The Information System Security Manager (ISSM) for each of our command/ activities maintains the information about his/her command or activity. Information system security posture may be either a "full" accreditation or and Interim Authority to Operate (IATO). The "full" accreditation is valid for three years, unless significant changes have been made within the three years. The IATO is valid for one year. The summary includes the date of the status. Additionally, the application provides a visual evaluation of the status. The following is the criteria for the visual evaluation:

SYMBOL	CRITERIA
	Current Full Accreditation
	Current Interim Authority to Operate (IATO)
	Accreditation (Full or IATO) will expire within 90 days
	One of the following: <ul style="list-style-type: none"> ▪ No accreditation information provided ▪ Expired accreditation ▪ IATO Pending ▪ Consecutive IATOs

The ISSM will post (in WORD (.doc) and/or Acrobat (.pdf) format) the following supporting information system security accreditation documents within the application:

- Appointment Letters (IT Manager, ISSM, NSO, etc.)
- Accreditation Letters (Full and/or IATO)
- Information System Security Plan (ISSP)
- CAP Waiver Letter

Maintenance of the Command s Information System Security Posture is an ongoing effort; as opposed to the semiannual AIS Security Report. As information changes, the data will be maintained.

Public Key Infrastructure (PKI). PKI is a framework of laws, policy, procedures and technology for the use of digital credentials, which provide:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation in electronic communications and transactions.

Risk Management. A process through which undesirable events can be identified, measured, controlled and prevented so as to effectively minimize their impact or frequency of occurrence. The *fundamental element of risk management* is the identification of the security posture (i.e., the characteristics of the functional environment from a security perspective). Risk management identifies the impact of events on the security posture and determines whether or not such impact is acceptable and, if not acceptable, provides for corrective action. Risk assessment, Security Test & Evaluation (ST&E) and contingency planning are parts of the risk management process.

Safeguards (aka countermeasures). These are the protective measures and controls that are prescribed to meet the security requirements specified for an information system, network or computer resource. Safeguards may include, but are not necessarily limited to, hardware and software security features, operational procedures, accountability procedures, access and distribution controls, management constraints, personnel security and physical structures, areas and devices.